and to improve clarity. No new matter is being added by virtue of the proposed amendment to the specification, and claims 1-30 remain pending.

The Applicant thanks the Examiner for granting telephone interviews and the appreciates the Examiner's assistance in resolving and clarifying certain issues during those interviews.

In item 9 (page 3), the Examiner rejected claims 1-30 under 35 U.S.C. § 103(a) as being unpatentable over Vogel (US Pat No 5,815,683) and further in view of Netscape version 2. The Examiner "notes" (in items 14-18) that Applicant's prior arguments are found unpersuasive and particularly notes that a roaming user and stored bookmarks, calendar data, pager numbers, etc., that were subjects of Applicant's prior arguments, are not claimed.

The Examiner tacitly admits that Vogel "fails to mention a single application other than CAD", but notes that "Vogel provides a user with access to different CAD tools." The Examiner further asserts that one of ordinary skill would have been motivated to first modify Vogel to incorporate access to multiple CAD packages, then to modify Vogel to provide the user with access to engineering databases, literature searches, financial reports, product development and the like, and then to further modify Vogel to provide access privileges varying from one service to another (item 19).

The Examiner also admits that Vogel is silent on selection of or providing access to such resources (items 22, 24) and tacitly admits that Vogel fails to teach or suggest providing secure client-server access (item 26), but reasons that the Internet is global (item 23), the availability of "selecting options" since the 80's (e.g. Netscape, Explorer and Visual Basic) would provide motivation to modify Vogel (item 25), and the existence of secure connections in other applications would provide motivation to further modify Vogel to provide encryption "to provide such a link" (item 27).

The Examiner also tacitly admits that Vogel fails to even mention providing client service communication codes (item 28) and does not teach a key safe not on the user system (item 30), but reasons that object oriented systems such as Visual Basic provide menus/buttons to implement services/options (item 29), and storage of keys on a user system could be a security

risk and keys are only needed by a system managing the access of resources (item 31).
Applicant respectfully traverses.

First, while the Applicant appreciates the Examiner noting that certain potential claims are not presently included and reserves the right to add them or others as might be appropriate, it is respectfully submitted that the included claims are no less patentable by such absence. Rather, certain of Applicant's prior arguments were made with regard to support provided by the Specification and were not intended as limitations (as was noted). It is possible, for example, that other than a roaming user, such as a user of a desktop PC or other stationary, mobile, more or less secure or other device, or a user not utilizing bookmarks, calendar data, pager numbers, etc. might also benefit from the teachings of the present invention or embodiments thereof.

Secondly, the failure of Vogler to teach or suggest embodiments recited in the rejected claims is clear even by the Examiner's own admissions. Further, even assuming arguendo that one or more of the asserted aspects might somehow be considered implementable, the degree to which Vogler would require modification is clearly substantial and the incentive to do so is clearly lacking.

For example, Vogler is apparently completely unconcerned with keys or certificates, or providing ANY extra-client security whatsoever. The Vogler system merely "prompts client 12 for client information ... through a pop-up window" which can further require "access facilitator's identification and a connection port". Access facilitator "waits for the prompted information to be entered and an indication from the user to submit the [user] entered information" and access facilitator "submits the entered information to access services 56." (Col. 4, lines 46-62.)

In contrast, the embodiment recited in independent claim 1 at least provides: "A system on a server computer system, comprising ... a keysafe for storing keys, each key for enabling communication between the client and a respective service from the set of available services, thereby enabling the client to access the available services without storing the... keys at the client."

Further, the embodiment recited in independent claim 15 at least contrastingly provides: "A computer-based method comprising... retrieving a key from a set of keys, each key corresponding to a respective service... the retrieved key for enabling communication between the client and the selected service...."

The embodiment recited in independent claim 29 also at least contrastingly provides: "A system on a server computer system, comprising ... means for retrieving a key from a set of keys, each key corresponding to a respective service ... the retrieved key for enabling communication between the client and the selected service ...."

The embodiment recited in independent claim 30 also at least contrastingly provides: "A computer-based storage medium storing a program for causing a computer to perform the steps of... retrieving a key from a set of keys, each key corresponding to a respective service... the retrieved key for enabling communication between the client and the selected service ...."

Third, while prior art deficiencies are expressed in the present Background of the Invention, these are clearly based on the observations of the *Applicant* and should not be imputed in impermissible hindsight to those of ordinary skill in the art at the time the Application was filed. Rather, Vogel clearly failed to teach or suggest at least security such as noted above and provided no incentive for doing so. It will further be shown that the cited prior art of Netscape and Internet Explorer also failed to teach, suggest, or provide any incentive whatsoever for the suggested combination, that the combination would not produce such security and that the cited references instead teach away from such security both alone and in combination.

More specifically, the cited prior art, other such systems, and even their *current* progeny store keys, certificates, username/password combinations, etc. within a client computer. The keys (or other security) are then selected by a client user for submission from the client to a resource as needed. For example, the Internet Explorer Help Screen "Protecting your identity over the internet" at the last paragraph of "How do certificates work" states: "Before you can start sending encrypted or digitally signed information, you must obtain a certificate and set up Internet Explorer to use it." It further states: "You can obtain your personal security certificate from certification authorities." (Emphasis is original). The Outlook Security options settings

window for specifying handling of user certificates stored on the <u>client</u> system also provides yet another example of saving keys/certificates at the <u>client</u> site. Such references are attached for the Examiner's convenience.

Fourth, neither Vogler nor the Netscape documentation provide <u>any</u> incentive for the suggested combination. Not only do Vogler and Netscape fail to teach or suggest the claimed embodiments, but Vogler employs <u>user</u> supplied information, has no services with which multiple security might be enabled, and fails to even mention using keys; Netscape requires a <u>client</u> to locally store and utilize its certificates. Thus, certainly the combination of the two would conflict with the rejected claims at least by also requiring such user/client supplied information.

Fifth, the embodiment recited in independent claim 1 at least provides "A system on a server computer system, comprising ... a keysafe for storing keys, each key for enabling communication between the client and a respective service from the set of available services, thereby enabling the client to access the available services without storing the... keys at the client." While the Examiner has admitted that the invention is useful by enumerating the benefits of storing the access codes and keys at a place other than the client (item 12), he apparently reasons that such usefulness is cause for rejection rather than a requirement of patentability. The Examiner further does so with impermissible hindsight, since the cited art has been available since the 80's (item 25) and <u>still</u> teaches user/client provided security, and not the teachings of the present invention.

For at least the above reasons, withdrawal of the rejections of claims 1, 15, 29, and 30 is respectfully solicited. The remaining rejected claims further depend from claims 1, 15, 29, and 30 and are patentable for at least the same reasons that claims 1, 15, 29, and 30 are patentable. Reconsideration of the rejections and early allowance of claims 1-30 is therefore respectfully requested.
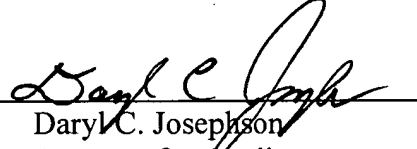
Attached hereto is a marked-up version of the changes made to the specification by the current amendment. The attached page is captioned **"Version with markings to show changes made."** Also attached are the aforementioned screens relating to Netscape and Outlook.

If the Examiner has any questions or needs any additional information, the Examiner is invited to telephone the undersigned attorney at (650) 843-8796.

If for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. 05-0150.
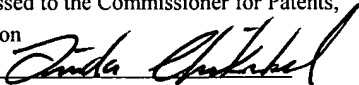
Respectfully submitted,

Dated: 4/17/01

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone (650) 856-6500
Facsimile (650) 856-3619

By _____
Daryl C. Josephson
Attorney for Applicants
Reg. No. 37,365

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, Washington, D.C. 20231, on

Date: 4/18/01 By: _____
Name of person signing certification

Version With Markings To Show Changes Made

In the specification:

Paragraph beginning at page 11 line 4 has been amended as follows:

--To enable user access to and control of the services 110a-110d, the global server 106 may use conventional applets, servlets or agents in a distributed network environment, such as Java™ distributed environment produced by the Netscape Corporation. The global server 106 provides the user's client with access to and control of the service 110a-110d. The global server 106 may redirect the user's client to access the service 110a-110d ~~itself~~, the global server 106 may access the service 110a-110d ~~itself~~ and provide I/O to the client by proxy, or the global server 106 may provide the service 110a-110d itself. These three different modes of access to the services 110a-110d are described with reference to FIGs 8A-8C.--

Hide   Back   Forward   Options   Web Help

Contents | Index | Search |

Type in the keyword to find:

Keys, private and public

Display

Protecting your identity over the Internet

You can use a personal certificate to protect your identity over the Internet. A certificate is a statement guaranteeing the identity of a person or the security of a Web site. You can control the use of your own identity by having the private key that only you know on your own system. When used with mail programs, security certificates with private keys are also known as "digital IDs."

Internet Explorer uses two different types of certificates:

- A "personal certificate" is a kind of guarantee that you are who you say you are. This information is used when you send personal information over the Internet to a Web site that requires a certificate verifying your identity.

- A "Web site certificate" states that a specific Web site is secure and genuine. It ensures that no other Web site can assume the identity of the original secure site.

How do security certificates work?

A security certificate, whether it is a personal certificate or a Web site certificate, associates an identity with a "public key." Only the owner knows the corresponding "private key" that allows the owner to "decrypt" or make a "digital signature." When you send your certificate to other people, you are actually giving them your public key, so they can send you encrypted information which only you can decrypt and read with your private key.

The digital signature component of a security certificate is your electronic identity card. The digital signature tells the recipient that the information actually came from you and has not been forged or tampered with.

Before you can start sending encrypted or digitally signed information, you must obtain a certificate and set up Internet Explorer to use it. When you visit a secure Web site (one that starts with "https"), the site automatically sends you their certificate.

Where do you get your own security certificates?

Security certificates are issued by independent certification authorities. There are different classes of security certificates, each one providing a different level of credibility. You can obtain your personal security certificate from certification authorities.

In   Microsoft Outlook:
Digital Certificates sit on users' PC
(Tools → options → security → settings)

Inbox - Microsoft Outlook

File Edit View Favorites To

New · | 🖨 | 🌐 ← · ·

Find | Organ

Outlook Shortcuts | **Inbox**

Folder List

Outloo

Inbo

Cale

Con

Ta

My Sh

Other S

23 Items

Options ? X

Preferences ● Services | Mail Format | Spelling | Security | Other ● egates |

Secure e-mail

☐ Encrypt contents and attachments for outgoing messages

☐ Add digital signature to outgoing messages

☐ Send clear text signed message when sending signed messages

Default Setting: [▼] Settings...

scripts and active
the Microsoft

Zone Settings...

Attachment Security...

allow you to prove your

Get a Digital ID...

Cancel | Apply

Change Security Settings ? X

Security Setting Preferences

Security Settings Name: [▼]

Secure Message Format: [S/MIME ▼]

☐ Default Security Setting for this Secure Message Format

☐ Default Security Setting for all secure messages

New | Delete | Password...

Certificates and Algorithms

Signing Certificate: [ ] Choose...

Hash Algorithm: [▼]

Encryption Certificate: [ ] Choose...

Encryption Algorithm: [▼]

☑ Send these certificates with signed messages

OK | Cancel

matter adverse to
ct to what we term
standards, this is
l and jumps ships,
lified no matter wh
e is some flexibili